

КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

2006

Печатается по решению учебно-методического совета
механико-математического факультета КГУ

Составители: доц. Корешков Н.А., асс. Насрутдинов М. Ф.

Содержание

1	Деление с остатком	4
2	Функции $[]$ и $\{ \}$	5
3	Некоторые основные теоретико-числовые функции	5
4	Умножение Дирихле и функция Эйлера	7
5	Цепные дроби	8
6	Теорема Эйлера и ее применение	9
7	Решение сравнений первой степени	10
8	Китайская теорема об остатках и системы сравнений первой степени	12
9	Решение сравнений. Сравнения по примарному модулю.	13
10	Евклидовы области	14
11	Квадратичные вычеты	15
12	Первообразные корни и индексы	17
	ЛИТЕРАТУРА	18

1 Деление с остатком

- 1.1. Найти наибольшее число, дающее при делении на 13 частное 17.
- 1.2. Доказать, что остаток при делении квадрата нечетного натурального числа на 8 равен 1.
- 1.3. Доказать, что сумма квадратов двух последовательных натуральных чисел при делении на 4 дает остаток 1.
- 1.4. Доказать, что если $a \equiv 1 \pmod n$ и $b \equiv 1 \pmod n$, то $ab \equiv 1 \pmod n$.
- 1.5. Доказать, что $3n + 2$ не может быть квадратом целого числа.
- 1.6. Доказать, что среди 5 последовательных натуральных чисел одно делится на 5.
- 1.7. Доказать, что сумма $2n + 1$ последовательных чисел делится на $2n + 1$.
- 1.8. Доказать, что $5|m^5 - m$.
- 1.9. Доказать, что $6|m^3 + 5m$.
- 1.10. Доказать, что $6|m(m + 1)(2m + 1)$.
- 1.11. Доказать, что $9|4^n + 15n - 1$ для любых положительных целых n .
- 1.12. Доказать, что если $m - p|mn + pq$, то $m - p|mq + np$.
- 1.13. Найти все натуральные n , для которых $n + 1|n^2 + 1$.
- 1.14. Найти все целые $n \neq 3$, для которых $n - 3|n^3 - 3$.
- 1.15. Доказать, что если $7|m^2 + n^2$, то $7|m$ и $7|n$.
- 1.16. Доказать, что в пифагоровой тройке один из катетов делится на 3.
- 1.17. Доказать, что в пифагоровой тройке одна из сторон делится на 5.
- 1.18. Доказать, что простое число $p > 5$ при делении на 6 дает остаток 1 или 5.
- 1.19. Доказать, что квадрат простого числа $p > 3$ при делении на 24 дает остаток 1.
- 1.20. Если трехзначное число делится на 37, то все числа полученные круговой перестановкой тоже делится на 37.

2 Функции $[]$ и $\{ \}$

Целой частью вещественного числа называется наибольшее целое число, не превосходящее x . Обозначение $[x]$ (читается "антье от x "). Дробной частью числа x называется число $\{x\} = x - [x]$.

Примеры. $[3.14] = 3$, $[-3.14] = -4$, $\{-3.14\} = 0.86$.

Теорема 2.1 Показатель, с которым простое число p входит в разложение $n!$ равен

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots + \left[\frac{n}{p^k}\right] + \dots$$

При этом лишь конечное число слагаемых в сумме не равно нулю.

2.1. Найти целые и дробные части следующих чисел: 3.14 , -4.1 , $\sqrt{35}$, $\sqrt{30} + \sqrt[3]{10}$

2.2. Построить графики функций $y = [x]$, $y = \{x\}$

2.3. Выразить $[x + y]$ через целые и дробные части x , y

2.4. Показать, что количество чисел кратных d , лежащих на отрезке $[1, x]$ равно $\left[\frac{x}{d}\right]$

2.5. Сколькими нулями оканчивается число $2006!$

2.6. Сколькими нулями оканчивается число $191!$

2.7. С каким показателем число 6 входит в произведение $100!$

2.8. С каким показателем степени простое число p входит в $(p^n)!$

2.9. Найти НОК всех натуральных чисел, не превышающих m .

3 Некоторые основные теоретико-числовые функции

Функция $\theta : \mathbb{N} \rightarrow \mathbb{C}$ называется мультипликативной, если (1) $\theta(a) \neq 0$ хотя бы для одного натурального a (2) для любых взаимно простых чисел a и b имеем $\theta(ab) = \theta(a)\theta(b)$.

Функцией Мебиуса называется функция $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$, определяемая условиями

$$\mu(a) = \begin{cases} 1, & \text{если } a = 1 \\ (-1)^n, & \text{если } a = p_1 p_2 \dots p_n, \text{ где все } p_i \text{ различные простые числа} \\ 0, & \text{если } a \text{ делится на квадрат простого числа} \end{cases}$$

Функция Эйлера $\varphi(a)$ определяется для положительных чисел и равна количеству чисел ряда $0, 1, \dots, a-1$ взаимно простых с a . По определению $\varphi(1) = 1$.

3.1. Какие из следующих функций $f(x)$ мультипликативны:

1. $f(x) = x^s$, где s любое вещественное (или комплексное) число;
2. $f(x) = \sin(x)$;
3. $f(x) = \lg(x)$.

В следующих задачах a – целое положительное число и $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ его каноническое разложение на простые множители.

3.2. Пусть $\theta(x)$ – мультипликативная функция. Доказать, что

$$\sum_{d|a} \theta(d) = (1 + \theta(p_1) + \dots + \theta(p_1^{\alpha_1})) \dots (1 + \theta(p_n) + \dots + \theta(p_n^{\alpha_n}))$$

3.3. Пусть $\theta(a)$ мультипликативная функция. Доказать, что $\theta_1(a) = \sum_{d|a} \theta(d)$ – мультипликативная функция.

3.4. Доказать, что $\sum_{d|a} d^s = (1 + p_1^s + \dots + p_1^{s\alpha_1}) \dots (1 + p_n^s + \dots + p_n^{s\alpha_n})$.

3.5. Доказать, что число делителей a равно $\tau(a) = (1 + \alpha_1) \dots (1 + \alpha_n)$.

3.6. Найти сумму делителей $S(a)$ числа a .

3.7. Найти сумму и число делителей числа 500.

3.8. Пусть θ мультипликативная функция. Доказать, что $\sum_{d|a} \mu(d)\theta(d) = (1 - \theta(p_1)) \dots (1 - \theta(p_n))$

3.9. Найти $\varphi(a)$ и $\mu(a)$ для чисел от 1 до 15.

3.10. Найти $\sum_{d|a} \mu(d)\varphi(d)$.

3.11. Найти $\sum_{d|n} \mu(d)$.

3.12. Найти $\sum_{d|n} \frac{\mu(d)}{d}$. (Применить теорему к мультипликативной функции $1/d$)

4 Умножение Дирихле и функция Эйлера

Пусть $f, g : \mathbb{N} \rightarrow \mathbb{C}$. Произведение Дирихле функций f и g определяется формулой

$$(f \circ g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

4.1. Доказать, что произведение Дирихле ассоциативно.

4.2. Определим функцию α равенствами $\alpha(1) = 1$ и $\alpha(n) = 0$ для $n > 1$.

Пусть $f : \mathbb{N} \rightarrow \mathbb{C}$ произвольная функция. Доказать $f \circ \alpha = \alpha \circ f = f$.

4.3. Определим функцию β равенствами $\beta(n) = 1$ для всех $n \geq 1$. Пусть $f : \mathbb{N} \rightarrow \mathbb{C}$ произвольная функция. Доказать $f \circ \beta = \beta \circ f = \sum_{d|n} f(d)$.

4.4. Доказать, что $\beta \circ \mu = \mu \circ \beta = \alpha$.

4.5. Формула обращения Мебиуса. Пусть $f : \mathbb{N} \rightarrow \mathbb{C}$ произвольная функция. Определим $F(n) = \sum_{d|n} f(d)$. Доказать, что

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right).$$

4.6. Доказать, что $\sum_{d|n} \varphi(d) = n$ (Гаусс).

(Рассмотреть числа $1/n, 2/n, \dots, n/n$, сократив числители и знаменатели, выяснить что означает количество чисел со знаменателем d .)

4.7. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$ каноническое разложение числа n . Доказать, что

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_l}\right).$$

4.8. Доказать, что $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, где $d = (m, n)$.

4.9. Найти все m , для которых $\varphi(m) = 4$.

5 Цепные дроби

Конечной цепной дробью называется выражение

$$\delta_n = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}}},$$

где $q_1 \geq 0$, $q_i > 0$ при $i > 0$ и $q_n > 1$. Будем сокращенно записывать цепную дробь в виде $\langle q_1, q_2, \dots, q_n \rangle$

Теорема 5.1 *Всякое рациональное число $\frac{a}{b} > 0$ разлагается в конечную цепную дробь. При этом q_i неполные частные в алгоритме Евклида вычисления (a, b) .*

Пусть $a = bq_1 + r_2$, $b = r_2q_2 + r_3, \dots, r_{n-1} = r_nq_n$. Тогда $\frac{a}{b} = \delta_n$.

Приводя к общему знаменателю можно записать δ_s в виде обычной дроби. Обозначим $\delta_s = \frac{P_s}{Q_s}$, где $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$. Тогда $P_s = q_s P_{s-1} + P_{s-2}$ и $Q_s = q_s Q_{s-1} + Q_{s-2}$; $(P_s, Q_s) = 1$.

Значения P_s и Q_s удобно вычислять с помощью таблицы

q_s		q_1	q_2	\dots	q_{n-1}	q_n
P_s	1	q_1	P_2	\dots	P_{n-1}	a
Q_s	0	1	Q_2	\dots	Q_{n-1}	b

Если $\alpha = \langle q_1, q_2, \dots, q_n \rangle$, то $|\alpha - \frac{P_s}{Q_s}| < \frac{1}{Q_s^2}$, при $s \leq n$.

5.1. Разложить в цепные дроби:

(a) $\frac{125}{92}$; (b) $\frac{127}{52}$, (c) 1, 23.

5.2. Свернуть непрерывные дроби:

(a) $\langle 1, 1, 2, 1, 2, 1, 2 \rangle$, (b) $\langle 0, 1, 2, 3, 4, 5 \rangle$.

5.3. Следующие числа заменить дробями с возможно меньшими знаменателями так, чтобы погрешность не превосходила 10^{-4} :

(a) $\frac{1261}{881}$; (b) $\frac{587}{103}$.

6 Теорема Эйлера и ее применение

Теорема 6.1 Чтобы $a^{\varphi(m)} \equiv 1 \pmod{m}$, необходимо и достаточно, чтобы $(a, m) = 1$.

6.1. Доказать, что любое нечетное целое число не кратное 5, в 12-той степени оканчивается на 1.

6.2. Доказать, что если $(a, 7) = 1$, то $7 | a^{12} - 1$.

6.3. Доказать, что если $(a, 65) = (b, 65) = 1$, то $65 | a^{12} - b^{12}$.

6.4. Пусть p – простое число. Доказать, что число вида $a^{p-1} + p - 1$, где $a \not\equiv 0 \pmod{p}$, является составным.

6.5. Пусть p – простое число. Доказать, что $(a + b)^p \equiv a^p + b^p \pmod{p}$.

6.6. Доказать, что наименьшее целое положительное x , удовлетворяющее сравнению $a^x \equiv 1 \pmod{m}$, где $(a, m) = 1$, является делителем числа $\varphi(m)$.

- 6.7.** Доказать, что натуральное число m не делящееся ни на 2, ни на 3, ни на 5 является делителем $\varphi(m)$ -значного числа вида $11 \dots 1$.
- 6.8.** Доказать, что если $\sum_{i=1}^n a_i \equiv 0 \pmod{30}$, то $\sum_{i=1}^n a_i^5 \equiv 0 \pmod{30}$.
- 6.9.** Доказать, что $p_1^{p_2-1} + p_2^{p_1-1} \equiv 1 \pmod{p_1 p_2}$, где p_1, p_2 — различные простые числа.
- 6.10.** Доказать, что если $(a, m) = 1$ и $\alpha_1 \equiv \alpha_2 \pmod{\varphi(m)}$, то $a^{\alpha_1} \equiv a^{\alpha_2} \pmod{m}$.

7 Решение сравнений первой степени

7.1. Пусть $m > 0$ фиксированное целое число, $a, b \in \mathbb{Z}$. Будем говорить, что a эквивалентно b ($a \sim b$), если $m | a - b$. Показать, что это действительно отношение эквивалентности.

7.2. Пусть $m > 0$ фиксированное целое число. Обозначим через $[a] = \{x \in \mathbb{Z} | m | (a - x)\}$ класс эквивалентных элементов относительно введенного выше порядка. Показать, что

1. $[a] + [b] := \{x + y | x \in [a], y \in [b]\} = [a + b]$.
2. $[a] \cdot [b] := \{xy | x \in [a], y \in [b]\} = [ab]$.
3. Показать, что $Z_m = \{[0], [1], \dots, [m - 1]\}$ кольцо относительно введенных операций.

Сравнение первой степени с одним неизвестным это сравнение вида

$$ax \equiv b \pmod{m}. \quad (1)$$

Теорема 7.1 (1) Если $(a, m) = 1$, то сравнение имеет единственное решение, которое находится по формуле

$$x \equiv a^{\varphi(m)-1} b \pmod{m}$$

или по формуле

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m},$$

где P_{n-1} числитель предпоследней подходящей дроби в разложении $\frac{m}{a}$ в цепную дробь.

(2) Если $(a, m) = d$, то сравнение имеет решение, только если $d|b$. При этом сравнение имеет d решений, которые находятся по формулам

$$x_k \equiv x_0 + k \frac{m}{d} \pmod{m},$$

$k = 1, 2, \dots, d-1$, а x_0 решение сравнения

$$\frac{a}{d} x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

7.3. Решить сравнения первой степени:

(a) $29x \equiv 1 \pmod{17}$; (b) $21x + 5 \equiv 0 \pmod{29}$;

(c) $6x \equiv 27 \pmod{12}$; (d) $8x \equiv 20 \pmod{12}$;

(c) $(a^2 + b^2)x \equiv a - b \pmod{ab}$, $(a, b) = 1$; (d) $ax \equiv 1 \pmod{p}$, p -простое и $p \nmid a$.

7.4. Решить в целых числах уравнения:

(a) $5x + 4y = 3$ (сводится к системе $5x \equiv 3 \pmod{4}$ и $4y \equiv 3 \pmod{5}$);

(b) $17x + 13y = 1$.

7.5. На прямой $8x - 13y + 6 = 0$ найти число целых точек, лежащих между прямыми $x = -100$ и $x = 100$.

7.6. Доказать, что внутри прямоугольника, ограниченного прямыми $x = -2$, $x = 5$ и $y = -1$, $y = 2$, на прямой $3x - 7y - 1 = 0$ не лежит ни одной целой точки.

8 Китайская теорема об остатках и системы сравнений первой степени

Пусть m_1, m_2, \dots, m_k – попарно взаимные простые числа, то система

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots \\ x \equiv c_k \pmod{m_k} \end{cases} \quad (2)$$

имеет решение, которое единственно по модулю $m = m_1 m_2 \dots m_k$.

Для решения системы необходимо найти y_1, y_2, \dots, y_k , удовлетворяющие сравнениям $\frac{m}{m_j} y_j \equiv 1 \pmod{m_j}$. Тогда решение имеет вид

$$x = \sum_{j=1}^k \frac{m}{m_j} y_j c_j.$$

8.1. Решить следующие системы сравнений

$$\begin{aligned} (1) \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 8 \pmod{11} \end{cases}; \quad (2) \begin{cases} 4x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{6} \end{cases}; \\ (3) \begin{cases} 17x \equiv 7 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 2x \equiv 2 \pmod{5} \end{cases}; \quad (4) \begin{cases} 3x \equiv 5 \pmod{7} \\ 2x \equiv 3 \pmod{5} \\ 3x \equiv 3 \pmod{9} \end{cases}. \end{aligned}$$

8.2. Найти все натуральные числа, делящиеся на 5 и дающие при делении на 2, 3, 4 в остатке 1.

8.3. (Старинная французская задача). Женщина несла на рынок корзину яиц. Прохожий нечаянно толкнул корзину и разбил яйца. Желая возместить ущерб, он спросил сколько было яиц в корзине. "Точно не помню, – ответила женщина, – но когда я раскладывала яйца по 2,3,4,5,6 яиц, то в корзине оставалось 1 яйцо, а когда по 7, то ничего не оставалось". Сколько было яиц?

8.4. Найти все значения a , при которых имеет решение система

$$\begin{cases} 2x \equiv a \pmod{4} \\ 3x \equiv 4 \pmod{10} \end{cases}$$

8.5. Найти хотя бы одно значение m , при котором не имеет решение система

$$\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 7 \pmod{m} \end{cases}$$

8.6. Найти целые точки прямых $4x - 7y = 9$, $2x + 9y = 15$ и $5x - 13y = 12$, лежащие на одном перпендикуляре к оси абсцисс.

8.7. Решить сравнение с двумя неизвестными (а) $x + 2y \equiv 1 \pmod{3}$; (б) $2x - y \equiv 1 \pmod{4}$.

8.8. Решить системы сравнений

$$(a) \begin{cases} x + 3y \equiv 5 \pmod{7} \\ 4x \equiv 5 \pmod{7} \end{cases}; (b) \begin{cases} 9y \equiv 15 \pmod{12} \\ 7x - 3y \equiv 1 \pmod{12} \end{cases}.$$

9 Решение сравнений. Сравнения по примарному модулю.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ многочлен с целыми коэффициентами.

Рассмотрим сравнение

$$f(x) \equiv 0 \pmod{m}.$$

Если $m = p$ — простое число, то сравнение равносильно сравнению $r(x) \equiv 0 \pmod{p}$ степени не выше чем $p - 1$, где $r(x)$ остаток от деления многочлена $f(x)$ на $x^p - x$.

Если $m = m_1 m_2 \dots m_n$, где m_i взаимно просты, то сравнение равносильно системе $f(x) \equiv 0 \pmod{m_i}$, $i = 1, \dots, n$.

Если $m = p^n$. То решение сводится к решению сравнений вида $f(x) \equiv 0 \pmod{p}$.

Последовательно находим x_1, x_2, \dots, x_n следующим образом:

x_1 – решение сравнения $f(x) \equiv 0 \pmod p$, при $f'(x_1) \neq 0$ находим $x_{i+1} = x_i + p^i t$, где t решение сравнения $\frac{f(x_i)}{p^i} + t f'(x_i) \equiv 0 \pmod p$.

Искомое x равно x_n .

9.1. Решить сравнения:

- (a) $x^2 + 2x + 2 \equiv 0 \pmod 9$;
- (b) $9x^2 + 29x + 62 \equiv 0 \pmod{64}$;
- (c) $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$;
- (d) $x^3 + 2x + 2 \equiv 0 \pmod{125}$;
- (e) $x^2 \equiv p \pmod{p^2}$.

9.2. Доказать, что сравнение $x^2 \equiv a \pmod 4$, где $(a, 2) = 1$, имеет решение тогда и только тогда, когда $a \equiv 1 \pmod 4$. Найти все решения сравнения при $a \equiv 1 \pmod 4$.

9.3. Доказать, что сравнение $x^2 \equiv a \pmod 8$, где $(a, 2) = 1$, имеет решение тогда и только тогда, когда $a \equiv 1 \pmod 8$. Найти все решения сравнения при $a \equiv 1 \pmod 8$.

9.4. Доказать, что сравнение $x^2 \equiv a \pmod{2^k}$, где $(a, 2) = 1$ и $k > 2$, имеет решение тогда и только тогда, когда $a \equiv 1 \pmod 8$. Доказать, что в этом случае существует ровно 4 решения.

10 Евклидовы области

10.1. Доказать, что следующие области не являются факториальными: $\mathbb{Z}[\sqrt{-5}]$; $\mathbb{Z}[\sqrt{-10}]$.

10.2. Показать, что следующие области являются евклидовыми:

- (a) $\mathbb{Z}[i]$; (b) $\mathbb{Z}[\sqrt{-2}]$; (c) $\mathbb{Z}[\sqrt{3}]$; (d) $\mathbb{Z}[\sqrt{6}]$.

10.3. Решить уравнения в целых числах.

- (a) $y^2 + 1 = x^3$;
- (b) $y^2 + 4 = x^3$;

(с) $y^2 = x^3 + 1$.

11 Квадратичные вычеты

Число a называется квадратичным вычетом по модулю простого нечетного числа p , если сравнение $x^2 \equiv a \pmod{p}$ имеет решение. В противном случае a называется квадратичным невычетом.

Символ Лежандра

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ квадратичный вычет} \\ -1, & \text{если } a \text{ квадратичный невычет} \end{cases}$$

Свойства символа Лежандра.

1. Если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$; $\left(\frac{b^2}{p}\right) = 1$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$; $\left(\frac{1}{p}\right) = 1$; $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
4. $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$, здесь q простое нечетное число.

Свойство 4 называется *законом взаимности квадратичных вычетов*.

11.1. Вычислить символ Лежандра: (а) $\left(\frac{13}{7}\right)$; (б) $\left(\frac{22}{13}\right)$; (с) $\left(\frac{426}{491}\right)$.

11.2. При помощи символа Лежандра выяснить, какие из следующих сравнений разрешимы:

- 1) $x^2 \equiv 5 \pmod{13}$; 2) $x^2 \equiv 5 \pmod{29}$
- 3) $x^2 \equiv 2 \pmod{97}$; 4) $x^2 \equiv 151 \pmod{587}$.

11.3. При помощи критерия Эйлера выяснить, какие из следующих сравнений разрешимы и найти соответствующие решения:

1) $x^2 \equiv -3 \pmod{7}$; 2) $x^2 \equiv 3 \pmod{11}$

3) $x^2 \equiv 6 \pmod{7}$.

11.4. Найти значения a , при которых имеют решения сравнения:

1) $x^2 \equiv a \pmod{3}$; 2) $x^2 \equiv a \pmod{5}$;

3) $x^2 \equiv a \pmod{7}$; 4) $x^2 \equiv a \pmod{11}$;

11.5. Доказать, что сравнение $x^2 + 1 \equiv p$ имеет решение тогда и только тогда, когда $p = 4n + 1$ ($n = 1, 2, 3, \dots$).

11.6. Доказать, что каноническое разложение чисел вида $a^2 + b^2$, где $(a, b) = 1$, содержит простые числа вида $p = 4n + 1$ ($n = 1, 2, 3, \dots$) и только такие простые числа.

11.7. Доказать, что произведение двух последовательных натуральных чисел при делении на 13 не может давать в остатке 1.

11.8. Доказать, что следующие сравнения разрешимы при любом простом $p > 2$:

(1) $(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod{7}$;

(2) $(x^2 - 3)(x^2 - 5)(x^2 - 7)(x^2 - 11)(x^2 - 1155) \equiv 0 \pmod{p}$.

11.9. Решить уравнения в целых числах (найти целые точки, через которые проходят кривые):

(1) $4x^2 - 5y = 6$; (2) $11y = 5x^2 - 7$; (3) $13y = x^2 - 21 + 110$.

11.10. Найти все такие простые числа p , что разрешимы сравнения:

1) $x^2 \equiv 5 \pmod{p}$; 2) $x^2 \equiv 2 \pmod{p}$

3) $x^2 \equiv -7 \pmod{p}$.

11.11. Вычислить $\sum_{x=2}^{p-1} \frac{x}{p}$

11.12. Существует ли такое n , что число $1 + 2 + \dots + n$ оканчивается на 7.

12 Первообразные корни и индексы

Пусть n положительное целое число, \mathbb{Z}_n кольцо вычетов по модулю n , $U = U(\mathbb{Z}_n)$ группа обратимых элементов кольца \mathbb{Z}_n .

Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, то $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$ и $U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{\alpha_1}}) \times U(\mathbb{Z}_{p_2^{\alpha_2}}) \times \dots \times U(\mathbb{Z}_{p_k^{\alpha_k}})$.

Порядок группы U равен $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$.

Теорема 12.1 Пусть n целое положительное число. Группа $U(\mathbb{Z}_n)$ циклическая группа при n равном $n = 2, 4, p^\alpha$ или $2p^\alpha$, где p простое нечетное число. В остальных случаях группа $U(\mathbb{Z}_n)$ не является циклической.

Число a , порождающее $U(\mathbb{Z}_n)$, называется примитивным корнем по модулю n .

Пусть $(a, n) = 1$. Говорят, что m порядок элемента a по модулю n , если m порядок элемента $\bar{a} = a + n\mathbb{Z}$ в группе $U(\mathbb{Z}_n)$. Будем писать в этом случае $o(\bar{a}) = m$.

Элемент a примитивный корень по модулю n тогда и только тогда, когда $o(\bar{a}) = \varphi(n)$.

12.1. Найти примитивные корни по модулю 11, 13, 17.

12.2. Показать, что 2 примитивный корень по модулю 29.

12.3. Показать, что если $p = 2^n + 1$ простое число Ферма, то 3 примитивный корень по модулю p .

12.4. Пусть a примитивный корень по модулю числа p^n (p простое). Доказать, что a примитивный корень по модулю p .

Примитивные корни по модулю p^k и $2p^k$.

Далее p простое нечетное число, $n = p^k$ или $n = 2p^k$. В этом случае $U(\mathbb{Z}_n)$ циклическая группа. Пусть g примитивный корень по модулю n и $(a, n) = 1$.

В этом случае $a = g^l$ для некоторого $1 \leq l \leq \varphi(n) - 1$. Число l называется индексом a по модулю n и обозначается $l = \text{inda} = \text{ind}_g a$. Индекс аналогичен понятию логарифма, при этом первообразный корень играет роль аналогичную основанию логарифма.

$$\text{ind}ab = \text{inda} + \text{ind}b$$

Для небольших p составлены таблицы индексов.

Теорема 12.2 Пусть $(m, \varphi(n)) = d$. Сравнение

$$x^m = a \pmod n$$

разрешимо тогда и только тогда, когда inda делится на d . В случае разрешимости сравнение имеет d решений.

Отметим, что сравнение $x^m \equiv a \pmod n$ эквивалентно $m \text{ind} x \equiv \text{inda} \pmod{\varphi(n)}$.

12.5. По таблице индексов найти индексы по модулю 41 следующих чисел: 27, 21, 2.

12.6. Составить таблицу индексов по модулю 11.

12.7. Пользуясь таблицей индексов решить сравнения:

(a) $x^{60} \equiv 79 \pmod{97}$;

(b) $x^{55} \equiv 17 \pmod{97}$;

(c) $x^{15} \equiv 46 \pmod{97}$.

Список литературы

- [1] Виноградов И.М. *Основы теории чисел* – М.:Наука – 1981. – 172 с
- [2] Айерленд К., Роузен М. *Классическое введение в современную теорию чисел.* – М.:Мир – 1987. – 428 с

- [3] Кудреватов Г.А. *Сборник задач по теории чисел.* – М.:Просвещение – 1970. – 128 с
- [4] *Задачи и упражнения по теории чисел. Часть 1* – Н. Новгород.:ННГУ – 1995. – 29 с
- [5] *Задачи и упражнения по теории чисел. Часть 2* – Н. Новгород.:ННГУ – 1995. – 32 с